

Nicole Galloway, CPA

Missouri State Auditor

City of St. Louis

Information Technology Services Agency

Report No. 2019-029

April 2019

auditor.mo.gov



Nicole Galloway, CPA
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the City of St. Louis - Information Technology Services Agency

| | |
|---------------------------------------|--|
| Security Controls | The ITSA has not implemented all necessary security controls, leaving ITSA technology assets at risk of inappropriate access, use, and disclosure. The ITSA has not fully established or documented the physical security policies and procedures necessary to ensure areas housing information technology resources are properly controlled, monitored, and restricted to only authorized individuals. The ITSA has not established internal policies and procedures to inventory certain ITSA-owned technology assets. |
| Vendor Security | The ITSA has not consistently ensured contracts for software acquired or outsourced from information technology vendors contain security requirements, or reviewed the security practices used by vendors. |
| Information System Control Activities | The ITSA needs to improve certain information system control activities. |

No rating will be given.

City of St. Louis - Information Technology Services Agency

Table of Contents

| | |
|------------------------|---|
| State Auditor's Report | 2 |
|------------------------|---|

| | |
|-----------------------------|---|
| Introduction | |
| Background | 4 |
| Scope and Methodology | 6 |

| | |
|---|----|
| Management Advisory Report - State Auditor's Findings | |
| 1. Security Controls | 8 |
| 2. Vendor Security | 10 |
| 3. Information System Control Activities | 11 |



NICOLE GALLOWAY, CPA

Missouri State Auditor

To the Honorable Mayor
and
Chief Information Officer
City of St. Louis, Missouri

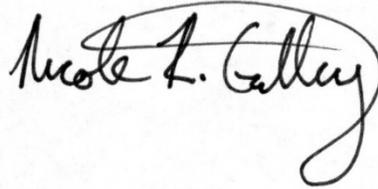
We have audited certain operations of the City of St. Louis Information Technology Services Agency (ITSA) in fulfillment of our duties under Section 29.200.3, RSMo. The State Auditor initiated audits of the City of St. Louis in response to a formal request from the Board of Aldermen. The city engaged KPMG LLP, Certified Public Accountants (CPAs), to audit the city's financial statements for the year ended June 30, 2018. To minimize duplication of effort, we reviewed the CPA firm's report. The scope of our audit included, but was not necessarily limited to, the year ended June 30, 2018. The objectives of our audit were to:

1. Evaluate the agency's internal controls over significant management operations and financial functions.
2. Evaluate the agency's compliance with certain legal provisions.
3. Evaluate the economy and efficiency of certain management practices and information system control activities.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides such a basis.

For the areas audited, we identified (1) deficiencies in internal controls, (2) no significant noncompliance with legal provisions, and (3) the need for improvement in management practices. The accompanying Management Advisory Report presents our findings arising from our audit of the City of St. Louis ITSA. Our audit also found the ITSA needs to improve certain information system control activities. We are not disclosing details of these issues in this report because of the sensitivity of the activities and to avoid compromising the confidentiality of the ITSA's resources. Instead, we communicated the issues confidentially to City of St. Louis and ITSA officials so they could take corrective action.

Additional audits of various officials and departments of the City of St. Louis are still in process, and any additional findings and recommendations will be included in subsequent reports.

A handwritten signature in black ink that reads "Nicole R. Galloway". The signature is written in a cursive style with a large, looping 'G' at the end.

Nicole R. Galloway, CPA
State Auditor

The following auditors participated in the preparation of this report:

| | |
|---------------------|---|
| Director of Audits: | Jon Halwes, CPA, CGFM |
| Audit Manager: | Jeffrey Thelen, CPA, CISA |
| In-Charge Auditor: | Alex R. Prenger, M.S.Acct., CPA, CISA, CGAP |
| Audit Staff: | Kent Aaron Dauderman, M.Acct., CPA, CGAP |

City of St. Louis - Information Technology Services Agency

Introduction

Background

The Information Technology Services Agency (ITSA) was established in 2003 under ordinance 65798, and is responsible for the planning, development, coordination and implementation of timely, reliable, cost-effective technology and information services for use by city government and city employees, citizens, and businesses. Duties include hardware, software and web support; network and server maintenance and security; and user account management for the network and certain information systems and applications.

The ITSA's role within the city's governance structure, and its overall service to all city employees, place the agency in the most direct position to guide citywide information security efforts. Weaknesses in those efforts are due in part to long-term challenges the ITSA has faced, and/or continues to face.

Director oversight

The ITSA's current director, who also serves as the city's Chief Information Officer, was appointed in December 2017. Prior to this appointment, the director position was vacant for 9 years. During this period, other city personnel were partially assigned to guide the ITSA, including one part-time director. However, their guidance was limited due to pre-existing duties and responsibilities. As a result, the ITSA lacked clear, dedicated direction in matters of information security policies and procedures.

The prolonged vacancy of a dedicated ITSA director also generally weakened communication between the ITSA and city departments. This issue resulted in situations when departments did not preemptively communicate with the ITSA before making major technology-related decisions and purchases.

Competing priorities

Prior to and following the current director's appointment, the ITSA faced other priorities requiring substantial attention and resources. These priorities included improving the city network resiliency, implementing information systems and applications for departments' use, creating and administering requests for proposal related to major technology projects, and designing other general security enhancements and controls. Certain tasks remained in progress as of January 2019.

Administrative relationship with departments

The city's organizational structure, and related factors presented below, cause the ITSA's administrative role to vary significantly by individual department.

- The ITSA and many departments are structured under and report to the Mayor's office. The ITSA's administration over such departments is often strong. Other departments are organized under standalone elected officials. The ITSA's administration over such departments is often weaker and less defined.
- The ITSA and certain departments operate under civil service rules administered by the Civil Service Commission and Department of



City of St. Louis - Information Technology Services Agency Introduction

Personnel. Other departments, typically those under standalone elected officials, are considered patronage departments. This affects certain aspects regarding broad ITSA policy distribution, enforcement, and discipline.

- Certain departments feature dedicated information technology personnel. While the ITSA communicates with these personnel, the departments often have greater autonomy to fulfill their unique technology needs.
- The ITSA does not directly administrate all forms of access to city networks, information systems, and applications. Certain instances are directly administrated by departmental personnel.

Of these challenges, the city's organizational structure will remain the most significant in the long term. A restructure of all departments' general information technology needs under the ITSA is beyond the scope of this audit. However, promoting communication and collaboration between the ITSA and departments, to the maximum degree feasible, will be critical towards the ITSA's efforts to establish information security policies and procedures in an increasingly consistent and effective manner.

Cyber threats continue to emerge and evolve

As connectivity of business activity increases and organizations become increasingly dependent on technology, including computerized systems and electronic data, no organization is exempt from cyber threats, vulnerabilities, and privacy exposures. As a result, it is important to view information security and privacy as a business issue rather than strictly an information technology issue. Security threats, vulnerabilities, and privacy exposures challenge every organization, creating data protection and privacy risks that must be understood, addressed, and managed.

The National Institute of Standards and Technology (NIST) defines cybersecurity as the process of protecting information by preventing, detecting, and responding to attacks¹ while ISACA states cybersecurity encompasses all that protects enterprises and individuals from intentional attacks, breaches, and incidents as well as the consequences.² Cybersecurity should be aligned with all other aspects of information security, including governance, management, and assurance. The state of being secure requires maintenance and continuous improvement to meet the needs of stakeholders and the demands of emerging cyber threats.

¹ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, is available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>, page 45, accessed February 11, 2019.

² ISACA, *Transforming Cybersecurity*, 2013, page 11.



City of St. Louis - Information Technology Services Agency
Introduction

The Government Accountability Office (GAO) has included the security of information systems since 1997, specifically adding the protection of Personally Identifiable Information (PII) in its 2015 update.³ Technological advances, such as lower data storage costs and increasing interconnectivity, have allowed both government and private sector agencies to collect and process extensive amounts of PII more effectively. Risks to PII can originate from unintentional and intentional threats. These risks include insider threats from careless, disgruntled, or improperly trained employees and contractors; the ease of obtaining and using hacking tools; and the emergence of more destructive attacks and data thefts.

Technology advances, combined with the increasing sophistication of individuals or groups with malicious intent, have increased the risk of PII being compromised and exposed. Correspondingly, the number of reported security incidents involving PII in both the private and public sectors has increased dramatically in recent years. At the same time, city governments are increasingly reliant on technology and information sharing to interact with citizens and to deliver essential services. As a result, the need to protect information, including PII, against cybersecurity attacks is increasingly important.

Security and privacy controls According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information. Effective privacy controls depend on the safeguards employed within the information system that is processing, storing, and transmitting PII and the environment in which the system operates. Organizations cannot have effective privacy without a basic foundation of information security. Without proper safeguards and controls, information systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

Scope and Methodology

The scope of our audit included evaluating (1) information security and other relevant controls, (2) policies and procedures, and (3) other management functions and compliance requirements in place during the year ended June 30, 2018.

³ Report GAO-17-157SP *Report to Congressional Committees, High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, March 2019, is available at <<http://www.gao.gov/assets/700/697245.pdf>>, accessed March 12, 2019



City of St. Louis - Information Technology Services Agency Introduction

Our methodology included reviewing written policies and procedures, and interviewing various ITSA personnel. We obtained an understanding of the applicable controls that are significant within the context of the audit objectives and assessed whether such controls have been properly designed and placed in operation. We tested certain of those controls to obtain evidence regarding the effectiveness of their design and operation. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, and we assessed the risk that illegal acts, including fraud, and violation of contract or other legal provisions could occur. Based on that risk assessment, we designed and performed procedures to provide reasonable assurance of detecting instances of noncompliance significant to these provisions.

We based our evaluation on accepted state, federal, and international standards and best practices related to information security controls from the following sources:

- National Institute of Standards and Technology (NIST)
- U. S. Government Accountability Office (GAO)
- ISACA

City of St. Louis - Information Technology Services Agency

Management Advisory Report

State Auditor's Findings

1. Security Controls

The ITSA has not implemented all necessary security controls, leaving ITSA technology assets at risk of inappropriate access, use, and disclosure.

1.1 Physical security

The ITSA has not fully established or documented the physical security policies and procedures necessary to ensure areas housing information technology resources are properly controlled, monitored, and restricted to only authorized individuals.

Physical security is the protection of technology resources, including computers and network servers, from theft or damage. Physical security makes technology resources physically unavailable to unauthorized users and can include locked rooms and cabinets, periodic inventories of technology assets, and other measures to protect assets from unauthorized access.

Physical security controls should be designed to prevent vandalism and sabotage, theft, accidental or deliberate alteration or destruction of information or property, attacks on personnel, and unauthorized access to computing resources, according to the GAO. Inadequate physical security could lead to the loss of property, the disruption of service and functions, and the unauthorized disclosure of data and information.

User access policies and procedures

The ITSA has not established policies and procedures for requesting, granting, and removing physical access to areas housing sensitive information technology resources.

Management should define and implement procedures to grant, limit and revoke access to premises, buildings, and areas according to business needs, including emergencies, according to accepted standards. Without appropriate procedures to grant and remove access to sensitive areas, individuals may receive inappropriate or unauthorized access.

Review of user access

The ITSA has not established procedures for independently reviewing physical access to sensitive information technology resources to ensure access rights are necessary to perform job responsibilities.

We reviewed system-generated reports of users with access to an area housing sensitive information technology resources. ITSA officials had not formally reviewed this area's access because they did not consider it high risk, access was limited to ITSA personnel, and no previous incidents of unauthorized access had occurred. However, our review found access was unnecessarily enabled for several current ITSA employees with incompatible duties, three previous ITSA employees who retired or resigned during 2017 and 2018, and one current city employee who was affiliated with the ITSA until early 2017. Following our review, ITSA officials indicated access would be appropriately restricted.



City of St. Louis - Information Technology Services Agency
Management Advisory Report - State Auditor's Findings

Agencies should periodically review the physical access granted to computer facilities and resources to ensure the access continues to be appropriate, according to the GAO. Without a formal documented review, physical access may be granted to or maintained for individuals who should not have access.

During our review, we also observed that one individual is responsible for activating and deactivating access, as well as handling blank, damaged, and returned access cards. To ensure integrity, periodic reviews should be independently completed by a separate individual.

1.2 Inventory

The ITSA has not established internal policies and procedures to inventory certain ITSA-owned technology assets. As a result, there is increased risk that the loss, theft, or misuse of such assets may go undetected.

All city departments are required to inventory assets costing at least \$5,000 to comply with Fixed Asset Management System (FAMS) policies and procedures established by the Comptroller's office. However, additional ITSA internal policies and procedures are needed to protect assets not covered by FAMS policies. Certain ITSA technology assets below the threshold, such as computers, laptops, and storage media, should be inventoried due to their portability, and potential misuse or data loss. Inventory records should be maintained on a perpetual basis, and include sufficient asset descriptions. Assets should be tagged to improve ITSA ownership identification and tracking. The ITSA should conduct periodic reconciliations and physical inventories.

Internal inventorying of certain ITSA assets costing \$5,000 or more may also be beneficial if more stringent or longer-term control is desired than existing FAMS requirements. A Comptroller's office internal audit report issued in October 2018, found that ITSA assets costing \$5,000 or greater were not always included in FAMS asset listings.

Recommendations

The ITSA:

- 1.1 Establish and document physical access policies and procedures, ensure access to sensitive technology assets is necessary with job responsibilities, implement independent periodic reviews of access, and timely remove unnecessary access.
- 1.2 Determine, through a risk assessment, which owned technology assets require protection; establish internal policies and procedures to inventory such assets; and conduct periodic reconciliations and physical inventories.

Auditee's Response

- 1.1 *The ITSA concurs our physical access policy was not fully documented. We now have a complete written policy in place that*



City of St. Louis - Information Technology Services Agency
Management Advisory Report - State Auditor's Findings

addresses both who should have access and how that access will be managed to ensure passes are deactivated promptly when necessary. The ITSA recently relocated some of the infrastructure that was located in the data center. We have now removed access from all personnel who no longer have reason to access the data center. Badges turned in by former employees have also been removed from the list of persons with access (Note: badges had been retrieved, but the roster did not reflect that fact).

- 1.2 *The ITSA concurs that we own assets (i.e., assets purchased by and issued to ITSA staff) that warrant better inventory control. The ITSA is now putting in place, through use of the asset management tool within our service ticketing system, procedures for tracking all items deemed to require stringent controls (regardless of the dollar value of the item). Procedures for tracking these assets are expected to be in place within the next 6 months.*

2. Vendor Security

The ITSA has not consistently ensured contracts for software acquired or outsourced from information technology vendors contain security requirements, or reviewed the security practices used by vendors.

The ITSA utilizes software products from a number of vendors to manage various city functions, including data backup and support services. Generally, the ITSA pays an annual licensing/maintenance fee for these products. Depending on the arrangement, some products are installed on city-owned equipment and maintained by ITSA personnel (with additional support from the vendor), while others are hosted and maintained directly by the vendor. In this case, city personnel access the system remotely, typically via a secure website.

We reviewed contracts for three systems or software products used by the city. Only one contract had a clause stating the vendor would provide appropriate security functionality for the city, as well as general descriptions of its security practices. In addition, the ITSA had not asked any vendors to provide documentation that their product's security functionality met generally accepted industry standards.

Accepted standards require organizations to identify and manage risk relating to a vendor's ability to securely deliver services; and when preparing contracts, to clearly define service requirements, including security and protection of intellectual property. Further security insight can be obtained by requesting independent reviews of vendor internal practices and controls, and/or reviewing vendor-supplied descriptions of security practices. Without consistently defining security requirements or assessing vendor security practices, the ITSA has less assurance in a vendor's ability to ensure services meet current and future data privacy and security needs.



Recommendation

The ITSA consistently ensure that vendor contracts contain security requirements, and review vendor security practices.

Auditee's Response

The ITSA agrees to the importance of ensuring vendor contracts contain security requirements and the need to review vendor security practices. We do wish to point out the ITSA oversees very few contracts that involve vendors having access to our data. Vendors who do have access to our data are well-known for meeting, if not setting, industry standards. Terms and conditions provided by these vendors, while not part of a specific agreement with the city, do attest to the vendors' security protocols. The ITSA in consult with our City Counselor's office, will immediately begin putting language into vendor contracts that more explicitly states what security requirements the vendor must meet and maintain, as well as explicitly states the city's right to review vendor security practices.

3. Information System Control Activities

The audit found the ITSA needs to improve certain information system control activities.

We are not disclosing details of these issues in this report because of the sensitivity of the activities and to avoid compromising the confidentiality of the ITSA's resources. Under Section 610.021.21, RSMo, a governmental body is authorized to close records to the extent the records identify and would allow unauthorized access or unlawful disruption of its computer, computer system, computer network, or telecommunications network.

During the audit, we communicated the issues and recommendations confidentially to City of St. Louis and ITSA officials so they could take corrective action.

Recommendation

The ITSA should implement the confidentially communicated recommendations for improving information system control activities.

Auditee's Response

The ITSA has already begun implementing and documenting the confidentially communicated recommendations.